CLAIMS

1. A method of authenticating a game data set for use in a casino-type gaming system, said method comprising the steps of:

(a) receiving the game data set;

(b) computing a primary abbreviated bit string unique to the game data set;

(c) encrypting the abbreviated bit string to provide a signature;

(d) storing the data set and the signature;

(e) computing a complementary abbreviated bit string from the stored data set;

(f) decrypting the stored signature to recover the primary abbreviated bit string;

(g) comparing the primary and complementary abbreviated bit strings to determine whether the primary and complementary abbreviated bit strings match;

(h) if the primary and complementary abbreviated bit strings match, indicating that the game data set is authentic; and

(i) if the primary and complementary abbreviated bit strings do not match, indicating that the game data set is not authentic.

2. A method of authenticating a game data set as recited in claim 1 wherein said step (b) of computing is performed with a hash function to produce a hash value of the game data set, and wherein said primary abbreviated bit string comprises the hash value of the game data set.

3. A method of authenticating a game data set as recited in claim 2 wherein the hash value comprises the message digest of the game data set.

4. A method of authenticating a game data set as recited in claim 1 wherein said step (c) of encrypting is performed using a private encryption key.

13. A method of authenticating a game data set as recited in claim 1 wherein said steps (a)-(d) are performed at a first site, and wherein steps (e)-(g) are performed at a second site.

14. A method of authenticating a game data set as recited in claim 13 wherein the first site comprises a manufacturing facility, and wherein said second site is a gaming facility.

15. A method of authenticating a game data set as recited in claim 1 wherein said game data set is a game-modifying data set for modifying game parameters of a casino type game.

16. A method of authenticating a game data set as recited in claim 15 wherein said game-modifying data set includes a money handler modifying data set for modifying parameters related to payout of coins and issuing of credit in the casino-type game.

17. A method of authenticating a game data set as recited in claim 15 wherein said game-modifying data set includes a sound driver modifying data set for modifying parameters related to sound drivers of said casino-type game.

18. A method of authenticating a game data set as recited in claim 15 wherein said game-modifying data set includes a graphics modifying data set for modifying parameters related to graphically displayed images of the casino-type game.

19. A method of preparing a casino game data set capable of authentication, said method comprising the steps of:

(a) providing a data set for a casino game;

(b) computing a primary abbreviated bit string unique to the casino game data set;

(c) encrypting the abbreviated bit string to provide a signature; and

(d) storing the casino game data set and the signature.

5. A method of authenticating a game data set as recited in claim 1 wherein said step (f) of decrypting is performed using a public decryption key.

6. A method of authenticating a game data set as recited in claim 1 wherein said step (c) of encrypting is performed using a private encryption key, and said step (f) of decrypting is performed using a public decryption key.

7. A method of authenticating a game data set as recited in claim 1 wherein said step (e) of computing is performed with a hash function to produce a hash value of the stored game data set, and wherein said complementary abbreviated bit string comprises the hash value of the stored game data set.

8. A method of authenticating a game data set as recited in claim 7 wherein the hash value comprises the message digest of the stored game data set.

9. A method of authenticating a game data set as recited in claim 1 wherein said step (d) of storing includes the step of storing the game data set and the signature in a mass storage device.

10. A method of authenticating a game data set as recited in claim 9 wherein the mass storage device comprises a disk drive unit.

11. A method of authenticating a game data set as recited in claim 9 wherein the mass storage device comprises a CD-ROM unit.

12. A method of authenticating a game data set as recited in claim 9 wherein the mass storage device comprises a network storage system.

20. A method of preparing a casino game data set as recited in claim 19 wherein said step (b) of computing is performed with a hash function to produce a hash value of the stored casino game data set, and wherein said primary abbreviated bit string comprises the hash value of the stored casino game data set.

21. A method of preparing a casino game data set as recited in claim 20 wherein the hash value comprises the message digest of the casino game data set.

22. A method of preparing a casino game data set as recited in claim 19 wherein said step (c) of encrypting is performed using a private encryption key.

23. A method of preparing a casino game data set as recited in claim 19 wherein said step (d) of storing the casino game data set and the signature includes storing the casino game data set and the signature in a mass storage device.

24. A method of preparing a casino game data set as recited in claim 23 wherein the mass storage device comprises a disk drive unit.

25. A method of preparing a casino game data set as recited in claim 23 wherein the mass storage device comprises a CD-ROM unit.

26. A method of preparing a casino game data set as recited in claim 23 wherein the mass storage device comprises a network storage system.

27. A method of authenticating a casino game data set of a casino type game having a signature encrypted from a primary abbreviated bit string computed from the casino game data set, said method comprising the steps of:

(a) computing a complementary abbreviated bit string from the casino game data set;

(b) decrypting the signature to recover the primary abbreviated bit string; and

(c) comparing the primary and complementary abbreviated bit strings to determine whether the primary and complementary abbreviated bit strings match.

28. A method of authenticating a casino game data set as recited in claim 27 wherein said step (a) of computing is performed with a hash function to produce a hash value of the casino game data set, and wherein said complementary abbreviated bit string comprises the hash value of the casino game data set.

29. A method of authenticating a casino game data set as recited in claim 28 wherein the hash value comprises the message digest of the casino game data set.

30. A method of authenticating a casino game data set as recited in claim 27 wherein said step (b) of decrypting is performed using a public decryption key.

31. In an electronic gaming system including a main memory, a first storage means having a first authentication program stored therein, a second storage means having stored therein an anchor application including a second authentication program, and an anchor signature including an encrypted version of a unique primary abbreviated anchor bit string computed from said anchor application, and a third storage means having stored therein a game data set and a game signature including an encrypted version of a unique primary abbreviated game bit string computed from said game data set, a method of authenticating game data sets for implementing casino-type games, said method comprising the steps of:

(a) loading said first authentication program stored in said first storage means to said main memory;

(b) accessing said anchor application stored in said second storage means;

(d) determining the validity of said anchor application using said first authentication program;

(e) if said anchor application is invalid, prohibiting the loading of said anchor application into said main memory;

(f) if said anchor application is valid,

loading said anchor application into said main memory,

accessing said game data set stored in said third storage means,

determining the validity of said game data set using said second authentication program,

if said game data set is invalid, prohibiting the loading of said game data set into said main memory,

if said game data set is valid, loading said game data set into said main memory and processing instructions of said game data set.

32. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said anchor application using said first authentication program includes the steps of:

computing a complementary abbreviated anchor bit string from said anchor application;

decrypting said anchor signature to recover said primary abbreviated anchor bit string;

comparing said primary and complementary abbreviated anchor bit strings to determine whether said primary and complementary abbreviated anchor bit strings match.

33. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program includes the steps of:

computing a complementary abbreviated game bit string from said game data set;

decrypting said game signature to recover said primary abbreviated game bit string;

comparing said primary and complementary abbreviated game bit strings to determine whether said primary and complementary abbreviated game bit strings match.

34. In an electronic gaming system as recited in claim 31 wherein said primary abbreviated anchor bit string is computed from said anchor application using a first hash function, and wherein said step of determining the validity of said anchor application using said first authentication program includes the steps of:

computing a complementary abbreviated anchor bit string from said anchor application using said first hash function;

decrypting said anchor signature to recover said primary abbreviated anchor bit string;

comparing said primary and complementary abbreviated anchor bit strings to determine whether said primary and complementary abbreviated anchor bit strings match.

35. In an electronic gaming system as recited in claim 34 wherein said primary abbreviated game bit string is computed from said game data set using a second hash function, and wherein said step of determining the validity of said game data set using said second authentication program includes the steps of:

computing a complementary abbreviated game bit string from said game data set using said second hash function;

decrypting said game signature to recover said primary abbreviated game bit string; and

comparing said primary and complementary abbreviated game bit strings to determine whether said primary and complementary abbreviated game bit strings match.

36. In an electronic gaming system as recited in claim 31 wherein said first storage means is an unalterable read only memory device.

37. In an electronic gaming system as recited in claim 31 wherein said second storage means is a mass storage device.

38. In an electronic gaming system as recited in claim 31 wherein said third storage means comprises a network storage system which is remote from the electronic gaming system.

39. In an electronic gaming system as recited in claim 31 wherein said electronic gaming system further includes a fourth storage means having stored therein a basic input/output operating system (BIOS) and wherein said first storage means further includes bootstrap code, an operating system, and operating system drivers stored therein, said method further comprising the steps of:

first loading said BIOS from said fourth storage means to said main memory; and

second loading said bootstrap code, said operating system, and said operating system drivers from said first storage means to said main memory, wherein said steps of first and second loading are performed before performing said step of loading said first authentication program.

40. In an electronic gaming system as recited in claim 31 wherein said first storage means is an unalterable read only memory, said second storage means is a mass storage means, and said third storage means is a mass storage means.

41. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatably initiated in response to initiation of game play.

42. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatably initiated in response to the detection of a coin insert.

43. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatably initiated in response to the payout of coins or issuing of credit.

44. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatably initiated by a demand procedure activated remotely from the gaming system via a network.

45. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatably initiated by a demand procedure activated locally at the gaming system.

46. In an electronic gaming system as recited in claim 31 wherein said gaming system further includes a fourth storage means having stored therein a game modifying data set and a game modifying signature including an encrypted version of a unique primary abbreviated bit string computed from said game modifying data set, said method further comprising the steps of:

accessing said game modifying data set in said fourth storage means;

determining the validity of said game modifying data set using said second authentication program;

if said game modifying data set is invalid, prohibiting loading of said game modifying data set into said main memory; and

if said second game data set is valid, loading said game modifying data set into main memory.

47. In an electronic gaming system as recited in claim 31 wherein said game data set is a game-modifying data set which includes a money handler modifying data set for modifying parameters related to payout of coins and issuing of credit in the casino-type game.

48. In an electronic gaming system as recited in claim 31 wherein said game data set is a game-modifying data set which includes a sound driver modifying data set for modifying parameters related to sound drivers of said casino-type game.

49. In an electronic gaming system as recited in claim 31 wherein said game data set is a game-modifying data set which includes a graphics modifying data set for modifying parameters related to graphically displayed images of the casino-type game.